PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-145219
(43)Date of publication of application : 26.05.2000

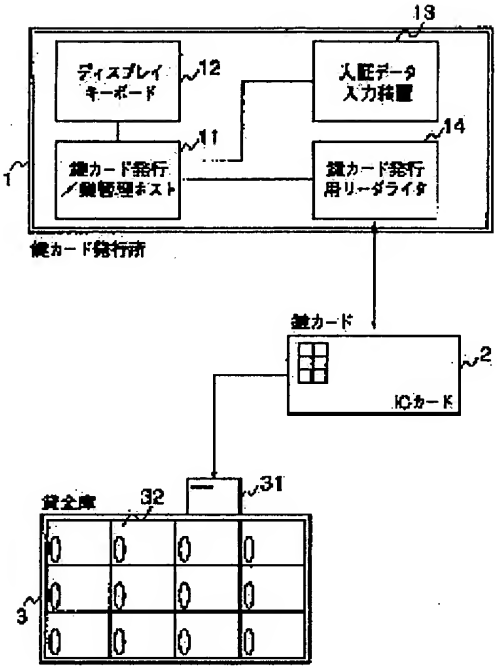
(51)Int.CI. E05B 49/00
E05B 65/00

(21)Application number : 10-323129
(22)Date of filing : 13.11.1998

(71)Applicant : HOKURA YUTAKA
(72)Inventor : HOKURA YUTAKA

(54) LOCK MANAGEMENT SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve safety severely judging a deserver by collating an inputted person proof data with an identical person certificated data of an IC card to unlatch and by using the IC card wherein the identical person certificated data of users is memorized as a key.
SOLUTION: A key card publishing house 1 is provided with a host computer 11, a data input device 12, an input device 13 for a person proof data, and a reader and writer 14 for publishing a key IC card. By a key card publishing house 1, a rental safe is specified, an ID for admitting utilization of the safe and an identical person certificated data of a user acquired with the input device 13 for a person proof data are stored in an IC card, the IC card is published as a key card 2, and the IC card is rented to a user. After a safe deposit box 3 is once locked, only when the person proof data wherein a user himself inputs in the scene is corresponded with the identical person certificated data read from the key card 2 which the user presents within a range admitted in collating theory, the safe is unlatched through an unlatching processor 31. Accordingly, the high safety of holdbacks can be secured.



LEGAL STATUS

[Date of request for examination] 13.11.1998
[Date of sending the examiner's decision of rejection] 27.06.2000
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－145219
（P2000－145219A）
(43)公開日　平成12年５月26日(2000.5.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ　49/00	Ｈ	２Ｅ２５０
65/00		65/00	Ｙ	

審査請求　有　　請求項の数８　ＯＬ　（全　６　頁）

(21)出願番号　特願平10－323129

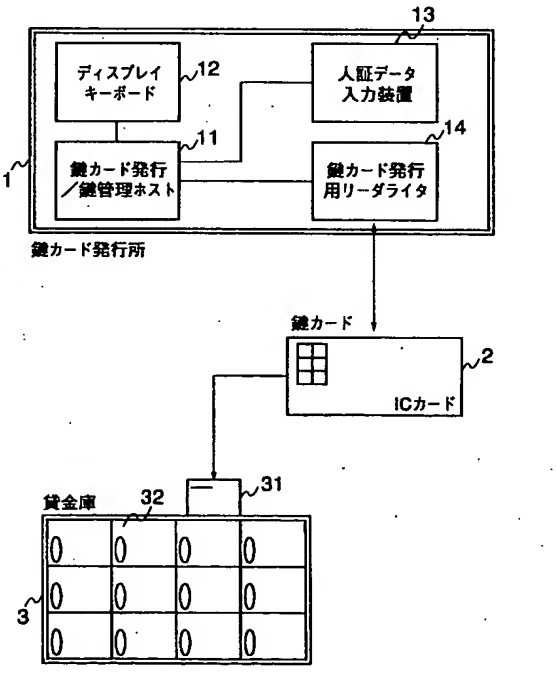
(22)出願日　平成10年11月13日(1998.11.13)

(71)出願人　398035796
保倉　豊
千葉県八千代市勝田台南２丁目15番22号
(72)発明者　保倉　豊
千葉県八千代市勝田台南２丁目15番22号
(74)代理人　100104341
弁理士　関　正治

Ｆターム(参考)　2E250 AA14 BB05 DD06 DD08 DD09
DD10 EE03 FF44

(54)【発明の名称】　錠前管理システム

(57)【要約】
【課題】　錠前にアクセスする資格者を厳格に判定して安全性が高い錠前管理システムを提供する。
【解決手段】　利用者の本人認証データを記録したＩＣカードを鍵として用い、利用時に入力される人証データとＩＣカードに記録された本人認証データを照合して認証に合格したときに電子錠を解錠する。



1

【特許請求の範囲】

【請求項１】　ＩＣカードリーダと人証データ入力装置を備え、利用者の本人認証データを記録したＩＣカードを前記ＩＣカードリーダで読み、前記人証データ入力装置から入力された人証データと前記ＩＣカードに記録された本人認証データを照合して認証に合格したときに対応する錠前を解錠することを特徴とする錠前管理システム。

【請求項２】　前記ＩＣカードに記録される本人認証データが、利用者が所有する生体情報データもしくは利用者が作成する情報データであることを特徴とする請求項１記載の錠前管理システム。

【請求項３】　前記ＩＣカードに記録できる本人認証データの種類が複数あって、選択して記録できることを特徴とする請求項１または２記載の錠前管理システム。

【請求項４】　前記人証データ入力装置が前記選択できる本人認証データの種類のうち少なくとも２種以上に対応して設置されていることを特徴とする請求項３記載の錠前管理システム。

【請求項５】　前記ＩＣカードにより解錠できる錠前が複数あって、それぞれについて適用する本人認証データの種類を選択することができることを特徴とする請求項３または４記載の錠前管理システム。

【請求項６】　前記錠前が金庫に設けられていることを特徴とする請求項１から５のいずれかに記載の錠前管理システム。

【請求項７】　前記錠前が複数の管理区分に分けられた保管庫の管理区分毎に設けられていて管理区分毎に適用する本人認証データが選択できることを特徴とする請求項３から５のいずれかに記載の錠前管理システム。

【請求項８】　前記管理区分に異物介入検知手段が設けられていて認証に合格した管理区分における前記検知手段の作動を停止させることを特徴とする請求項７記載の錠前管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、金庫や保管庫など許可した特定の者にのみ開閉を許すようにして、保管された重要物、薬品、毒物などの安全を保証する錠前の管理システムに関し、特に錠前に管理者を置かずに予め認可された者が自身で開閉するようにした錠前管理システムに関する。

【０００２】

【従来の技術】従来、貸ロッカーなどではロッカー毎に鍵を準備しこれを貸与する方式であるため、鍵を所有する者が本来の利用者と異なる場合でもロッカーの開閉ができるので、保管物が他人に盗取られる可能性があり、安全性は十分でない。より高度な保護を行う貸金庫などでは、金庫を貸すときに提供した鍵と管理者の鍵と合わせて始めて解錠できるようにしたものがあるが、管理者

2

が同席する必要があるうえ、盗まれたり複製された鍵を用いても解錠でき安全性も十分ではない。

【０００３】また、錠前に入力するダイヤルやキーボードを設けて、ロックするときに暗号を決めて同じ暗号を入力しなければ解錠できないようにした金庫もある。こうした金庫類では鍵を持ち歩く必要がなく、使用者が利用の度に設定する暗号に基づいて解錠するので、簡単でありながら安全性が高いが、暗号を盗み見たり類推により解錠される可能性が残る。さらに、研究室、資料保管室、薬品保管庫など、セキュリティの確保のため出入りできる者を限定し、有資格者に発行したカードによる認証に合格したときだけ解錠する錠前管理システムもあるが、このシステムではカードの管理が杜撰であると無資格者がカードを使用して自由に出入りするようになる畏れがある。

【０００４】なお、アクセスする錠前により要求されるセキュリティの程度が異なるため、何でも高い安全性を追求して利用者に煩雑な手続を要求することは避けなくてはならない。たとえば猛毒物を管理する棚を開けるためには多少煩雑でも確実な認証を必要とするが、持ち出し量を管理することで十分な通常の薬品を取り出すためには簡単な確認で十分である。貸金庫でも掛替えのない貴重品や高価な財物を収納したときと、いくらでも手に入る品物を収納したときでは、安全保証の要求水準が異なる。

【０００５】

【発明が解決しようとする課題】そこで、本発明が解決しようとする課題は、有資格者を厳格に判定して安全性が高い錠前管理システムを提供することであり、また必要に応じて有資格者認証の深さを設定できる錠前管理システムを提供することである。

【０００６】

【課題を解決するための手段】上記課題を解決するため、本発明の錠前管理システムは、利用者の本人認証データを記録したＩＣカードを鍵として用い、入力された人証データとＩＣカードに記録された本人認証データを照合して認証に合格したときに解錠することを特徴とする。

【０００７】本発明の錠前管理システムでは、錠前の使用を認めた者の本人認証データをＩＣカードに格納して、そのＩＣカードを鍵カードとして使用者に与える。錠前を解錠するときには鍵カードを提示すると共に人証データを入力する。この人証データを鍵カードに記録されたデータと照合して許容範囲内で合致しているときに始めて錠前を開ける。アクセスしようとする者の人証データが記録された本人データと合致していなければ錠前を開けることができないから、錠前は認可を受けた者にしか解錠することができない。

【０００８】このようなシステムは、認定を受けた個人に解錠する権限を与え、その資格を有する本人であるか

否かを鍵カードで認証するものであって、鍵カードは鍵機能の一部を担うに過ぎない。したがって、他人が鍵カードを拾得、盗取あるいは複製して使用しても、本人でない限り錠前を開けることができないため、錠前の安全性は極めて高い。また、本人情報は鍵カードに格納されているので、錠前装置側に利用予定者全員に関する情報を格納した大量のデータベースを備える必要も、ホスト装置から高速通信により取り寄せる必要もない。ただし、本人情報の一部を錠前側の記憶装置に格納して、両者を併せて用いるようにすれば、より高い安全を確保することができることは言うまでもない。

【０００９】なお、鍵カードに記録される本人認証データとして、利用者が所有する生体情報データもしくは利用者が作成する情報データを使用することができる。生体情報データとは、指紋、声紋、虹彩等、人体に備わっていて個人に特有の特徴を表す情報に関するデータをいう。このようなデータは、他人が成り済まして提示することが困難であるから、生体情報データに基づいて本人認証を行うことにより、錠前の安全性はより高くなる。

【００１０】また、利用者が作成する情報とは、署名や筆跡、あるいは任意の図形や文字列など本人が意図的に作成する情報をいう。署名等は人体に初めから備わるものではないが、生体情報と同じように他人がその特徴を真似することが困難なもので本人を正しく認証することに役に立つ。なお、文字列は鍵カードに格納され暗証番号と同じように使用されるが、ＩＣカードの記憶容量が大きいため長さや使用文字種などの自由度を拡大して他人が容易に推測できないようにすることができる。

【００１１】さらに、鍵カードに記録できる本人認証データの種類が複数あって、選択して記録できるようにしてもよい。鍵ＩＣカードを他人が盗用しようとしても、鍵カードが扱う認証データの種類を特定できないようになっていれば、指紋、声紋、署名、暗号などのいずれを使用しているかを知らなければ使えないのでカードを盗んでも役に立たず、盗難カードでの被害も減少する。

【００１２】また、複数の本人認証データ種類に対応する人証データの入力手段を錠前の利用場所に設置しておいて、利用者が選択できるようにしてもよい。このように複数の認証データ種類が利用できる場合は、盗用者はどの種類の認証データを使っているかを知る必要があり、安全性の高い錠前が得られる。勿論、複数の情報を併用していずれについても合格しなければ解錠できないようにしてもよい。

【００１３】なお、１枚の鍵カードにより解錠できる錠前が複数あって、それぞれについて適用する本人認証データの種類を選択することができるようにしてもよい。錠前毎に鍵カードを発行するよりコストが低減すると共に、利用者が携帯するカードの数を節減しかつ錠前毎に対応するカードを選んで提示する煩わしさを省くことができる。

【００１４】このような鍵カードは、さらに、たとえば保管庫で入口の錠と庫内の仕訳棚の錠を共用する場合などに有用である。保管庫内に管理水準の異なる通常薬品の戸棚と劇薬戸棚を設置してあるときに、保管庫の扉を開ける権限だけでは劇薬戸棚を開けられないようにすることができる。保管庫内に人事情報と経理情報を共に収納してあるがそれぞれ関係者のみしかアクセスできないようにするというような場合にも利用することができる。

【００１５】なお、このような状況では有資格者以外のアクセスがあった場合に警報する機能を付属すると安全性が向上する。このため、庫内の戸棚に人のアクセスを検知するセンサを設けることができる。センサは有資格者がアクセスする場合は作動する必要がないから、認証を合格した管理区分におけるセンサ回路については警報出力を禁止するようにしておく。

【００１６】無資格者がアクセスした場合は管理室に警報すると共に、保管庫の扉を閉じてそのアクセス者の逃亡を防ぐように構成しても良い。また、本発明の錠前管理システムでは錠前にアクセスした者を個人として認識する機能を有するので、その情報を集積することにより保管庫の利用状況記録を自動的に作製することができる。

【００１７】本発明の錠前管理システムは、貴重品を保管する金庫に設けて安全を図ることができる。特に貸金庫に利用することにより、管理者側の立ち会いがなくても十分安全な貸金庫設備となる。また、貸金庫利用者自身が、収納物の貴重度に応じてセキュリティの深度を決めてそれに応じた利用をすることも可能である。

【００１８】

【発明の実施の形態】以下、図面を参照して本発明の詳細を実施例に基づいて説明する。図１は本発明の錠前管理システムの１実施例の構成を示すブロック図、図２は別の実施例の構成を示すブロック図である。

【００１９】

【実施例１】本実施例の錠前管理システムは、貸金庫管理に利用したもので、ＩＣカード内に登録された認証データを用いて本人認証を行うことにより、高い安全性を備えることができる。図１を参照すると、鍵カード発行所１は貸金庫利用希望者に所定のＩＣカードを鍵カード２として発行し、貸金庫３は鍵カード２と利用者自身の認証データを読み取って認証に合格したときに鍵カード２が指定する金庫を解錠する。

【００２０】鍵カード発行所１は、ホストコンピュータ１１、ディスプレイやキーボードからなるデータ入出力装置１２、人証データ入力装置１３、鍵ＩＣカード発行用リーダライタ１４を備えている。金庫を借りたい者が利用を申し込むと、鍵カード発行所１の人証データ入力装置１３から利用者の認証に使用する人証データを入力させる。

5

【００２１】ホストコンピュータ１１には、ソフトウエアとして鍵カード発行ソフトウエア、鍵管理ソフトウエア、認証データ登録ソフトウエアを搭載してある。鍵管理ソフトウエアは金庫の使用状況を把握し鍵カードに対応させる金庫を決めたり、錠前のセキュリティレベルを管理し認証情報の種類を指定するなどのほか、鍵カードの発行返却状況を管理し返却された鍵カードの記録内容を確実に抹消する。データ入出力装置１２はコンピュータシステムで通常必要とされるディスプレイ、キーボード、プリンタなどから構成される。

【００２２】人証データ入力装置１３は、指を押し付けると指紋パターンを抽出して分類する指紋読み取り器、マイクロフォンと声紋解析装置からなる声紋取得器、サインや符号を書き込むタブレット、など利用者個人が識別できる情報を入力する装置である。簡単な場合は、文字列暗号を入力するキーボードであっても良い。鍵カード発行用リーダライタ１４は、ＩＣカードリーダライタとＩＣカードリーダライタコマンドから構成される。

【００２３】鍵カード発行所１は、貸す金庫を指定し、その金庫の利用を認める認証ＩＤと人証データ入力装置１３で取得した利用者個人の本人認証データをＩＣカード内のＣＰＵで管理されるメモリ領域に格納して、鍵カード２として発行し、利用者に貸与する。鍵カード２はＣＰＵと内蔵メモリを備えたＩＣカードである。

【００２４】貸金庫３には、ＩＣカードリーダライタと人証データ入力器を備えた解錠処理装置３１と複数のロッカー式金庫３２が設けられている。解錠処理装置３１は金庫制御インタフェースを備え認証データ照合ソフトウエアを搭載している。金庫３２は電気コントローラ付きで遠隔操作により施錠解錠ができる。なお、異常を検知するセンサと異常時に警報を発生する通報装置を設備しておくと無人化しても安全を確保することができる。

【００２５】貸金庫利用者は、貸金庫３のうちの指定された金庫３２に物を収納して施錠する。一旦施錠した後は、利用者本人がその場で入力する人証データと利用者が提示する鍵カード２から読み取った認証データとが照合論理上認められた範囲内で一致している場合に限り、解錠処理装置３１を介してその金庫を解錠する。

【００２６】本管理システムによれば、鍵カード２が真正なものであってもそれを携帯している者が真正な利用者でなければ解錠することができないので、金庫の安全性が高く、管理人の立ち会いなどによる保証を併用するまでもない。したがって、貸金庫装置を無人管理あるいはそれに近い管理により運営することも可能となる。

【００２７】なお、複数種類の認証情報を用いることにより、貸金庫のセキュリティレベルを選択して設定することも可能である。セキュリティレベルを選択できるようにしたものでは、金庫の利用者が金庫に収納する物の重要度と使い勝手を勘案して使用する認証情報を選択する。利用者が高いセキュリティを要求するときは署名により本人であることを確認することにしてもよいし、簡便さを重視した要求には文字列を使用すると決めても良い。

6

【００２８】さらに、照合すべき情報を２種以上の組み合わせにすることにより極めて安全性の高い金庫とすることも可能である。また、鍵カード２の発行時に利用する金庫を決めて、これに対応するＩＤをＩＣカード内に記入するようにすれば、未発行のＩＣカードが盗難にあっても盗用される危険は少ない。

【００２９】同じ錠前管理システムは、集中型セイフティボックスやロッカー、あるいは建物管理におけるキーボックスなど複数の者がアクセスする収納装置に利用することができる。

【００３０】

【実施例２】本実施例の錠前管理システムは、保管庫の管理に利用したもので、ＩＣカードと手書きサインによる照合で本人確認を行い、保管庫内の重要物、薬品・劇物・毒薬などを安全に保管し、許可された者が許可された物だけを取り出せるようにするシステムである。また、権限の無い者がアクセスしたときはセンサが検知して通報し、また外部からの攻撃にはシステムを安全サイドにロックするように回路構成を行うなど、保管庫の安全性と信頼性を十分に高める機能が付けられる。

【００３１】図２は、保管庫に適用した錠前管理システムのブロック図である。保管庫５は複数の保管室５１，５２，５３に分かれており、保管室５１内にさらに複数の小部屋あるいは保管棚５４，５５，５６がある。複数ある保管室それぞれと小部屋それぞれはセキュリティレベルが異なり、保管する物品の機密度に応じて保管室や小部屋を選別して使用することができる。

【００３２】具体的な例を挙げると、たとえばある会社で保管庫５を所有していて、第１保管室５１は社内でも一部の者にしか扱えない機密性の高い書類を保管する部屋とし特定の者にしか出入りを認めない。さらに、最高機密を要求される書類は第１保管室５１中の第１の小部屋５４に格納し、第１保管室５１に出入りが認められる者の中でも、さらに第１小部屋５４に入ることが認可される者しかアクセスさせない。また例えば第２小部屋５５は人事関係資料を格納する部屋で、人事担当の責任者しかアクセスが認められず、第３小部屋５６は経理書類の保管をする部屋で経理部の担当者しか出入りすることができないようにする。

【００３３】また、第２保管室５２は開発関係の資料を保管する部屋で、保管されている情報が外部に漏洩しないようにする必要があり、担当部局の者しか出入りさせない。一方、第３保管室５３は、重要度の低い文書を収納しておく部屋で、社員であれば誰でも出入りできるが、出入りの記録が残るようにする。また、セーフティボックス５７のように独立した保管庫も同じシステムで管理することができる。

【００３４】本実施例の保管庫管理システムでも第１の実施例におけると同様に、各保管室、各小部屋ごとに資格を決め、これに合致する社員に対してＩＣカードで作成する鍵カード２を給付する。鍵カード２に基づく本人認証により資格を認められた社員だけが認められた部屋の解錠を行うことができるようにする。すなわち、鍵カード２にはアクセスを認める錠前を指定する情報と人証データ入力装置で取得し所定の情報処理をした本人認証データがＩＣカード内のＣＰＵで管理されるメモリ領域に格納されている。

【００３５】また、保管庫５には、鍵カード２を読み取るＩＣカードリーダライタ４２と人証データ入力装置としてのタブレット４３と情報を交換できる制御ユニット４１、および各保管区分の錠前を制御するインターフェース４４を備える錠前管理装置４が設けられている。保管室５１，５２，５３や小部屋５４，５５，５６、またセーフティボックス５７の扉には遠隔で操作できる電気錠が設備されていて、錠前管理装置４により施錠解錠の制御が行われる。なお、各扉には異常検知センサ５８が設備されていて、部屋にアクセスがあると検知して信号を錠前管理装置４に送信する。また、表示灯を設備しておきアクセスを認めた扉のところで点灯して、アクセス者に知らせるようにしても良い。

【００３６】保管庫５を利用しようとするときは、利用者は鍵カード２をカードリーダライタ４２に挿入してタブレット４３に自分が登録時に決めた符号を入力する。制御ユニット４１は、鍵カード２が真正なＩＣカードであることを確認し、どの錠前に対応するものかを、鍵カード２のＣＰＵを介して提供される記録内容から確認する。次にタブレット４３から入力されたサインなどの人証情報を鍵カード２から提供される本人認証データと照合して同一であるかどうかを判定する。認証データ照合ソフトウエアにより両者が合致することが確認されたときに、鍵カード２が指定する錠前についてアクセス権を有する人物と判定して、指定した錠前を解錠する。

【００３７】使用者が許可された管理領域以外にアクセスするとセンサが作動して警報を発生する。不正アクセスがあったときは、錠前が自動的に施錠されて不正アクセス者を室内に閉じ込めるようにしても良い。なお、鍵カード２に基づいて解錠が許可されたときに、錠前または部屋や棚に設けられた表示灯の点灯により許可された対象を表示して、善意の者が誤ったアクセスをすることを防止するようにしても良い。

【００３８】対象とする部屋のセキュリティの高さにより要求する認証の深さを予め決めておくことができる。単に鍵カード２を提示すればアクセスを認める水準であってもよく、予め入力した符号と形状、筆順、筆圧が一致することを要求しても良い。また、暗証番号とサインなど複合した保証を要求するより高度な水準であってもよい。なお、これらの異なる水準のセキュリティに対応して複数の認証情報を１枚の鍵カード２に格納しておいて、アクセスする錠前毎に対応する認証データを読み出して照合するようにしても良い。

【００３９】さらに、保管庫５の側に複数の異なる人証データ入力手段を備えておいて、必要とする認証の水準により使い分けることもできる。一般に高いセキュリティレベルに対応する認証情報は人証データ入力に手間が掛かるため、低度の安全性しか要求しない錠前ではより簡単な認証方法を用いて使用者の便宜を優先することもできる。また、複数の種類から的確な認証情報を選択させることにより不正アクセスを排除しやすくすることもできる。どの種類の人証データをどの様に組み合わせるかを使用者自身に選択させるようにすると、他人の成り澄ましがさらに困難になり安全性がより向上する。

【００４０】また、本管理システムでは錠前にアクセスする個人が明確に把握できるので、いつ、誰が、どの保管室（あるいは保管棚等）にアクセスしたかを自動的に記録しておくことができる。なお、停電した時や電源ケーブルが切断されたときには、システムは機密上安全側にロックされるようになっている。保管庫を破壊行為などを含め異常が起こったときには管理室に警報する機構を備えることが好ましい。なお、緊急時にはロックを解除できる管理者用の認証レベルを備えておくことが好ましい。本実施例の説明は、書類の管理について記載したが、薬品を危険度に従って管理する薬品庫、薬品棚やロッカーなどの要求に対しても全く同じ実施例を適用することができる。

【００４１】

【発明の効果】以上詳細に説明した通り、本発明の錠前管理システムは、予め許可された人間自身しか錠前の解錠ができないようにするシステムで、認可された人物の認証を正しく行うため、保管物の高度の安全が確保できる。このシステムを適用することにより従来より安全度の高い保管庫管理システムや貸金庫管理システムを構築することができる。

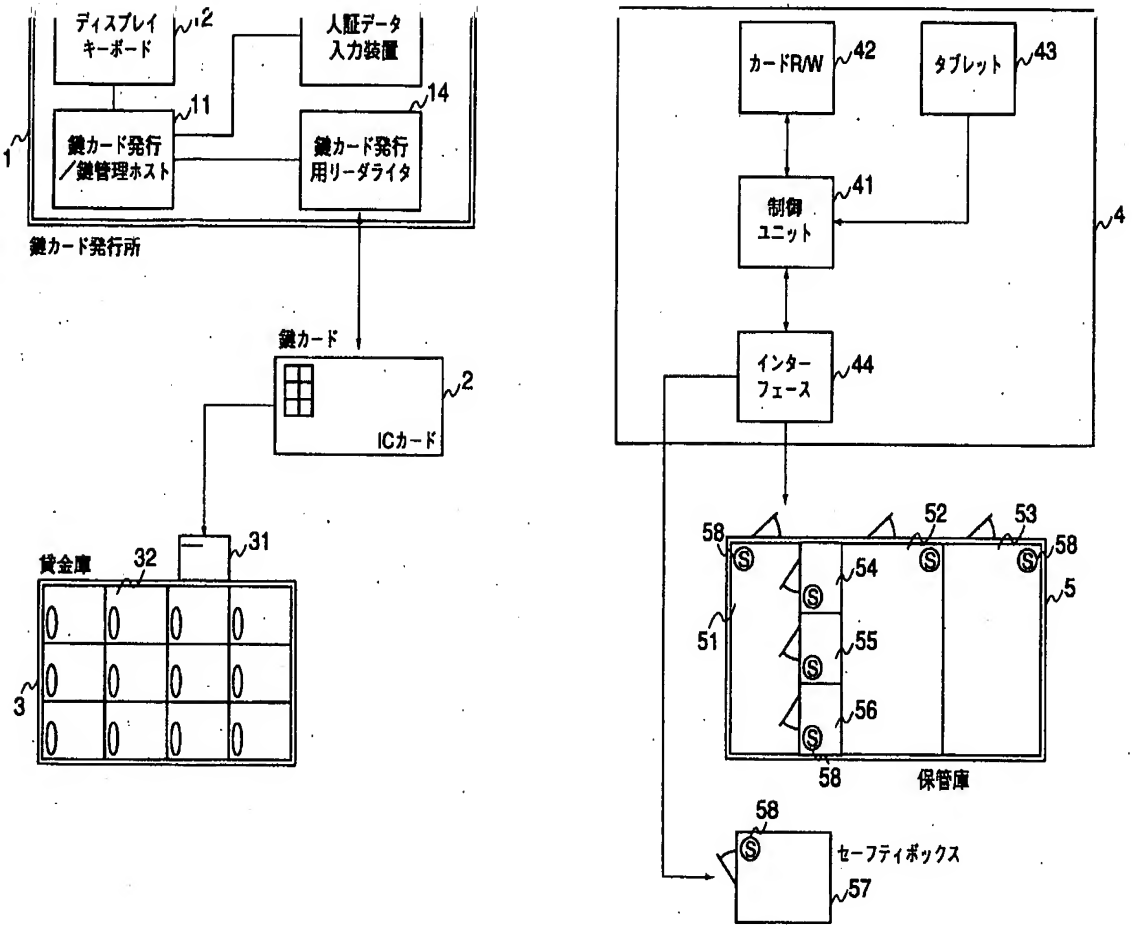
【図面の簡単な説明】

【図１】本発明の錠前管理システムの第１の実施例を示すブロック図である。

【図２】本発明の錠前管理システムの第２の実施例を示すブロック図である。

【符号の説明】

１　鍵カード発行所
１１　ホストコンピュータ
１２　データ入出力装置
１３　人証データ入力装置
１４　鍵ＩＣカード発行用リーダライタ
２　鍵カード
３　貸金庫
３１　解錠処理装置
３２　金庫


ディスプレイ
キーボード
12
人証データ
入力装置
11
14
1
鍵カード発行
／鍵管理ホスト
鍵カード発行
用リーダライタ
鍵カード発行所
鍵カード
2
ICカード
貸金庫
32
31
3
カードR/W
42
タブレット
43
制御
ユニット
41
4
インター
フェース
44
58
52
53
54
51
55
56
5
保管庫
セーフティボックス
57